Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report
for 07 April 2003

Daily Overview

- WUSA TV9 reports that every large commercial plane flying in the United States will have reinforced bulletproof cockpit doors by the middle of the month. (See item 5)

- IDG News Service reports the latest release of Apache 2.0 fixes a number of security vulnerabilities including an as−yet−undisclosed flaw that could be used to launch a denial of service attack against machines running the Apache Web server. (See item 20)

- Security News Portal reports three−quarters of web sites running Microsoft's Internet Information Server 5.0 software to serve web pages have the WebDAV protocol enabled, and thus remain open to a serious vulnerability which was announced by Microsoft last month. (See item 21)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: High
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://esisac.com]

1. *April 03, The Patriot−News, Harrisburg, PA* — **Nuclear power plant security evaluated. The level of security that owners of nuclear power plants are required to provide to protect their reactors from terrorist attacks may increase significantly, and at great cost, under plans being developed by the Nuclear Regulatory Commission (NRC).** The NRC will not discuss the plans, but industry and watchdog groups say there are indications the NRC will require extensive upgrades. "Generally, from what I hear, . . . some of the things floated . . . to

date really rise to the level that all of us in the industry look to the federal government to provide," said Steve Kerekes, spokesman for the Nuclear Energy Institute, an industry group based in Washington, D.C. "They are beyond the capability of many state and local law enforcement agencies, much less private industry." Kerekes would not attach a cost figure to any of the proposals. However, David Lochbaum of the Union of Concerned Scientists said he has been told that **the new security measures could cost the industry $30 million per plant, plus an additional $8 million to $10 million a year for additional guards.** If those numbers are accurate, it would cost Exelon Nuclear, which owns half of the Three Mile Island, Peach Bottom and Oyster Creek (N.J.) plants, plus seven other nuclear stations, about $245 million. And those expenses would be in addition to the $370 million the nuclear industry already has spent on security upgrades since the Sept. 11, 2002, terrorist attacks. **Included in the post–Sept. 11 costs are various capital improvements, such as fencing and barriers, and the addition of 2,000 security officers, a 35 percent increase, Kerekes said.** Security requirements for nuclear plants like Three Mile Island are set by the NRC. They are based on threat assessments issued by the State Department, intelligence agencies and the military. The policy, known as the Design Basis Threat, has not been changed significantly since 1993.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3750456

2. *April 02, The Day, New London, CN* — **Connecticut nuclear plant wants more federal funds for storage of spent fuel .** The Connecticut Yankee Atomic Power Co. said Tuesday that it is seeking more money from the federal government to cover the increasing cost of storing spent nuclear fuel at its decommissioned plant. **The company submitted a claim to the U.S. Court of Federal Claims Friday and is asking the court to increase the amount of damages from $112 million to $197 million.** In 1999, Connecticut Yankee filed with the court for the original $112 million after the Department of Energy failed to move the spent fuel at the site in 1998, as it was supposed to under a congressional mandate. **Since then the cost of keeping the spent fuel at the site has increased, particularly because of security measures required by the federal government after the Sept. 11, 2001 attacks.** "The costs are escalating so we filed a new claim," said Kelley Smith, a spokeswoman for the company. "Everything associated with fuel storage has increases since Sept. 11." In 1982, Congress passed a law to create a national nuclear waste storage site that would begin accepting nuclear waste by 1998. Last year, Congress approved the creation of the Yucca Mountain storage facility in Nevada, but the site will not likely open until 2010 at the earliest.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3750639

3. *April 02, Las Vegas Review – Journal* — **DOE looks at Yucca options.** Spurred by shrinking budgets, the Department of Energy (DOE) is reconsidering its strategy to ship nuclear waste to a planned repository at Yucca Mountain via railroad in Nevada. **Energy Department managers could postpone plans to build a rail spur within the state to the Yucca site, 100 miles northwest of Las Vegas. Instead, they may explore the temporary use of tractor–trailers that would transport waste in overweight shipping containers.** A shift in strategy from rail to truck, at least for initial years of repository operations, was among ideas discussed at a March 27 meeting where Energy Department managers looked for cost savings within the Yucca Mountain Project, a spokesman confirmed Monday. Analysts said shelving the Nevada rail spur could delay up to $1 billion in costs. The Energy Department already has delayed the formation of a transportation strategy, concentrating instead on preparing a license application. **Department officials say budget cuts by Congress, including a 22 percent reduction this**

year, have spurred cost reviews and could lead the department to postpone a December 2004 license application target.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3750991

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

4. *April 04, USA TODAY* — **Maryland airport evacuated after passenger sets off detector, walks away. Two concourses at Baltimore–Washington International Airport were evacuated for about an hour Thursday after a woman set off a metal detector and refused to be screened again. Instead, she walked away, and screeners didn't catch her, said federal Transportation Security Administration spokeswoman Heather Rosenker.** Authorities closed the checkpoint and the two concourses it serves, and planes that already had loaded passengers from the concourses were held at the gates, she said. Arriving flights were directed to other gates, said BWI spokeswoman Melanie Miller. Three flights remained delayed after the concourses reopened, officials said. Miller said she didn't know how many passengers were re–screened while the concourses were closed.
Source: http://www.usatoday.com/news/nation/2003–04–03–bwi_x.htm

5. *April 04, WUSA TV9* — **Airlines will meet deadline for reinforced cockpit doors.** Every large commercial plane flying in the United States will have bulletproof cockpit doors by next week, but airline security experts say the design doesn't provide the best possible protection against a hijacker entering. **The Federal Aviation Administration requires that cockpit doors be locked during flight, according to agency spokesman Les Dorr. But there are times when a pilot may open the door – to visually check wing surfaces, use the bathroom and change flight crews during a long trip. That leaves the possibility the cockpit could be rushed by a hijacker.** "It's a barrier when it's closed, it's an entry when it's open," said Capt. Steve Luckey, chairman of the Air Line Pilots Association's national security committee. The need to open cockpit doors was one reason pilots lobbied for guns in the cockpit, Luckey said.

Under a test program, about 48 pilots will be begin training to carry weapons while flying commercial passenger planes this month. Thousands more could be carrying weapons by the end of the year.
Source: http://www.wusatv9.com/news/news_article.asp?storyid=16741

[Return to top]

Postal and Shipping Sector

6. *April 04, Portsmouth Herald* — **New caucus on ports' security needs. Increasing communication between involved agencies and assuring funds are available for security to the nation's ports will be the focus of a new caucus group headed by a Maine legislator.** Senator Susan Collins chairman of the Governmental Affairs Committee, which oversees the U.S. Department of Homeland Security, has announced she will co−chair the Congressional Port Security Caucus. The caucus will focus on the security needs of the nation's ports. **The bicameral, bipartisan organization currently has 85 members, representing the top 33 U.S. ports in terms of foreign tonnage imports.**
Source: http://www.seacoastonline.com/news/04042003/news/21171.htm

7. *April 02, Bureau of Transportation Statistics* — **More than 10 percent of U.S. freight is from international trade.** More than 10 percent of the 16 billion tons of freight moved on the nation's transportation system is international freight, either entering the country as imports or intended for export, according to International Trade and Freight Transportation Trends, a new report released today by the U.S. Department of Transportation's Bureau of Transportation Statistics (BTS). **Almost 71 percent of the international freight tonnage in 2001 was from imports up from 65 percent in 1997 and the remaining 29 percent from exports.**
Source: http://www.dot.gov/affairs/bts0403.htm

[Return to top]

Agriculture Sector

8. *April 04, AgWeb* — **War impact on cattle difficult to predict.** Kansas State University agriculture economist James Mintert says fallout from the war in Iraq on the cattle markets is difficult to predict. But he says it could be minimal, unless the conflict widens. **"Fortunately, early indications are that the war has had little impact on either domestic or international meat demand, although declines in airline bookings could portend future declines in demand from hotels, restaurants and other institutions," he adds.** Meanwhile, Mintert says despite all the negative news reports about the U.S. economy, early signs from this winter indicate beef demand is improving.
Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsArticle_2003441032_3512newscat=GN

[Return to top]

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

Nothing to report.

[[Return to top](#)]

Public Health Sector

9. *April 06, CNN* — **WHO targets SARS "super spreaders". As the death toll from Severe Acute Respiratory Syndrome (SARS) mounts, the World Health Organization (WHO) says the key to controlling the mystery disease could lie in identifying highly infectious people, known as "super spreaders".** A WHO team is visiting hospitals and talking with experts in the southern Chinese province of Guangdong, which borders Hong Kong, where the SARS epidemic is thought to have originated. The four–member team is most interested in "the phenomenon of 'super spreaders' –– people who seem to spread their disease to a lot of other people," Associated Press reports WHO team leader Dr Robert Breiman saying. Figuring out why they are so infectious "may lead to public health approaches that will be very effective for control," he said. **Worldwide, the number of SARS cases continues to climb with over 2,400 infections and 89 deaths reported from 18 countries, WHO says. The 2,416 cases now reported represent an increase of 63 cases (2.7 percent) and five deaths (6.0 percent) in a 24 hour period.** Meanwhile, a vaccine is being developed by the United State's National Institutes of Health. Research is focusing on a suspected link between SARS and the coronavirus, which causes the common cold, according to The Associated Press news agency.
Source: http://www.cnn.com/2003/HEALTH/04/06/sars/index.html

10. *April 04, Sunday Mail* — **Masks "no protection from SARS". Surgical and cheap masks won't provide sure–fire protection against Severe Acute Respiratory Syndrome (SARS), a health expert warned Friday. But they could slow the spread of the disease by limiting hand to face contact.** "Surgical masks are designed to keep wounds sterile during surgery when a surgeon talks or coughs," Griffith University respiratory protection specialist Dr David Bromwich said. "They are not designed to protect the wearer." Dr Bromwich said the material used, and the fit of the masks, would offer almost no respiratory protection from airborne particles. **Scientists have said the virus is spread by droplets, through coughing and sneezing. But the World Health Organisation now believes it may also be spread by the environment, such as by water or sewerage systems, not just by close personal contact.**
Source: http://www.thesundaymail.news.com.au/common/story_page/0,593 6,6236401%255E421,00.html

11. *April 04, New York Times* — **An early warning system for diseases in New York City. In March, a corner of Queens suffered a sudden, sharp increase in the number of people with fever and trouble breathing, turning up mostly at one hospital's emergency room. Where a statistical analysis said there should have been 7 such cases over three days, there were 23.** The next day, there were 47. Suspecting an outbreak of the new Asian

respiratory disease, a team of city health workers fanned out. It turned out to be a false alarm, a statistical anomaly brought on by conditions as disparate as kidney stones and asthma. **What was remarkable about that episode was not so much the city's response, but that it was detected at all. No one at the hospital noticed it. Rather, the increase was caught by a computer at the New York City Department of Health and Mental Hygiene's headquarters where a statistical analysis program warned that there was only a 1 in 1,000 chance of such a thing being a random occurrence.** This was the work of the city's Syndromic Surveillance System, which public health experts call the most advanced early warning system for possible disease outbreaks in the country.
Source: http://www.nytimes.com/2003/04/04/nyregion/04WARN.html

12. *April 04, E4engineering.com* — **Biological weapons sensor detects anthrax in two minutes. A safer and faster way of detecting biological weapons agents has been devised by UK researchers with support from the UK's defence research agency.** The optical sensor, developed at University of Manchester Institute of Technology (UMIST) with the help of the Defence Science and Technology Laboratory, is designed to detect changes in antibodies when they come into contact with samples of deadly bacteria such as anthrax. It can also be used to detect bacteria that can lead to food poisoning. **Existing detection devices based on the use of antibodies tend to have low sensitivity, at least 10 million bacteria cells have to be present in 1ml of sample to produce a detectable signal. But levels as low as 10 cells per millilitre can cause infection, making the devices dangerous to use. The UMIST device can operate with a much smaller sample size, said Dr Mohammed Zourob of the university's department of instrumentation and analytical science, who developed the sensor with Dr Nicholas Goddard.**
Source: http://www.e4engineering.com/item.asp?id=48391ont>

13. *April 03, Associated Press* — **New TB blood test shows promise. Scientists have developed a new diagnostic test for tuberculosis that experts say could help control the disease in the developed world by more accurately detecting infections before people get sick.** The World Health Organization estimates that two billion people are infected with the bacteria that cause TB. The disease kills 2 million people a year. About 10 percent of people progress from a latent, or inactive, infection to the disease, but doctors cannot predict who or when. People can transmit the bug only when they get sick, so picking up infections early helps stop the spread. **A study indicates that the new test detected latent infections more accurately than the standard skin–prick test used for a century.**
Source: http://www.newsday.com/news/nationworld/wire/sns–ap–new–tb–t est.story

[Return to top]

Government Sector

14. *April 06, New York Times* — **New signs of terror not evident.** After U.S. government officials and many American lawmakers predicted that terrorist attacks were nearly inevitable because of the war in Iraq, there has been little evidence that al Qaeda or other networks are preparing to strike against the United States, senior government officials say. **As a result, intelligence analysts are turning their attention to a new potential threat, the likelihood that a protracted American presence in Iraq after the war could stir violence both in Iraq, the**

rest of the Middle East, in the United States and against American interests around the globe. A long and unpopular American occupation in Iraq could further inflame the already strong anti−American sentiments in the Arab world, causing extremist groups to engage in terrorist acts, the officials said. **Still, terror organizations like al Qaeda appear to have been largely unmoved by Saddam Hussein's denunciations of the United States and his calls for an uprising in the Arab world against the American−led war in Iraq.** One senior intelligence official said he had seen very little credible evidence that any terrorist plots were imminent in the United States.
Source: http://www.nytimes.com/2003/04/06/international/worldspecial /06SECU.html

15. *April 04, Government Executive* — **FBI designing vast terrorism database.** The FBI is testing a limited version of an electronic counterterrorism system that officials hope will revolutionize the way agents collect and understand information, FBI officials said Thursday. **As part of an ongoing technology upgrade, the FBI is building a massive database to store case information, leads, intelligence and even newspaper and magazine articles related to terrorism. Articles, the names of suspected terrorists on watch lists and terrorism−related message traffic from the Defense Department and the CIA have been placed into the database, which is being tested by some agents, according to Wilson Lowery, the FBI executive assistant director leading the project. Visa information from the State Department will be added to the database within 60 days, he said.** Lowery and a number of bureau officials briefed reporters on the new database, known as TID, or Terrorism Intelligence and Data. If designed as envisioned, it would house information from a vast array of sources and would be used in some capacity by the Terrorist Threat Integration Center, the government's new terrorism intelligence hub overseen by the CIA.
Source: http://www.govexec.com/dailyfed/0403/040303h1.htm

16. *April 04, Washington Post* — **FBI picks another outsider for key post.** The FBI announced on Thursday the appointment of a new top executive from the National Security Agency, marking the latest example of the continued influx of outside officials into the traditionally insular bureau. **Maureen S. Baginski, who is currently signals intelligence director at the NSA's Central Security Service, will become the highest−ranking woman at the FBI as executive assistant director for intelligence, officials said.** The new position was created by FBI Director Robert S. Mueller III as part of an effort to improve the collection and analysis of information on suspected terrorists and spies. **In addition, the FBI's counterterrorism division will soon move to a new location, along with the CIA's counterterrorism operations and the new Terrorist Threat Integration Center, which was formed by President Bush to collect and analyze all information about major threats against the United States.** The FBI also announced on Thursday the appointment of Steven C. McCraw to head the bureau's Office of Intelligence under Baginski. McCraw, a 20−year FBI veteran who heads the San Antonio field office, previously oversaw the FBI's massive database effort to track suspected terrorists.
Source: http://www.washingtonpost.com/wp−dyn/articles/A23513−2003Apr 3.html

17. *April 04, Washington Post* — **Historic Philadelphia sites to reopen with tighter security.** Independence Hall, closed by the National Park Service this week when city officials insisted on reopening the street in front of it, will open its doors again Friday with new security measures in place, federal officials said. **Although the Park Service and Homeland Security**

Secretary Tom Ridge had urged Mayor John Street to keep the street closed for security reasons, it was reopened Tuesday for the first time since shortly after the Sept. 11, 2001, terrorist attacks. Closing the street to vehicles and pedestrians had caused traffic problems in downtown Philadelphia, and merchants said it had harmed business. But officials at Independence National Historical Park said reopening the street forced them to temporarily close three historic buildings, including Independence Hall, where the Declaration of Independence was adopted and where the Constitutional Convention was held. The park had been using an area across the closed street for security screenings of visitors to the buildings. There is now a temporary screening area on the same side of the street as Independence Hall, and a permanent building is planned, a park spokesman said today.
Source: http://www.washingtonpost.com/wp−dyn/articles/A23454−2003Apr 3.html

18. *March 01, Department of Homeland Security* — **Statewide template initiative – Homeland Security Advisory Council.** The Template was built by state and local officials – those responsible for preventing, responding to, and recovering from the spectrum of terrorist threats and Homeland Security challenges that face the Nation in the 21st Century. **The Template provides a common foundation for identifying and addressing key state and local vulnerability and capability shortfalls.** Read the Statewide Template Initiative – Homeland Security Advisory Council http://www.dhs.gov/interweb/assetlibrary/Statewide_Template_Initiative.pdf
Source: http://www.dhs.gov/dhspublic/display?content=548

[Return to top]

Emergency Services Sector

19. *April 07, Federal Times* — **FEMA adjust programs, personnel to homeland role.** Transitioning into the new Homeland Security Department presents two big challenges to the Federal Emergency Management Agency. **One is adjusting its mission and programs to a new priority: ensuring the preparedness of the nation's first responders for terrorist attacks, major disasters and other emergencies. The other is the administrative and bureaucratic challenge of attaching itself to a new, large organization.** Federal Emergency Management Association (FEMA) had been an independent agency until March 1 when it formally joined Homeland Security. Now FEMA is the centerpiece of the department's Emergency Preparedness and Response Directorate, which also consists of preparedness and response organizations from five other federal agencies. But because the Homeland Security Department reorganization is barely a month old, most details have yet to be worked out. FEMA's managers, employees and the many first−responder organizations it deals with across the country still await word on what the reorganization will mean to them. **The directorate will dispense grants to first responders and will provide command and control in times of crisis, consolidate plans for federal responses to disasters or terrorist attacks, and align emergency response efforts under one roof, Homeland Security Secretary Tom Ridge told state emergency managers February 24.**
Source: http://federaltimes.com/index.php?S=1741611

[Return to top]

Information and Telecommunications Sector

20. *April 03,* — **Latest Apache release fixes DOS vulnerability. The latest release of Apache 2.0, version 2.0.45, fixes a number of security vulnerabilities including an as–yet–undisclosed flaw that could be used to launch a denial of service attack** against machines running the Apache Web server, according to information released by the Apache Software Foundation (ASF). **Apache 2.0 users are encouraged to upgrade**. Other, lower priority security leaks and bug fixes were also included in the 2.0.45 release. However, **a known DOS vulnerability that affects those systems running Apache on the OS/2 platform remains open**. The latest Apache version was "too important" to delay release until the OS/2 fix could be included, the ASF said. OS/2 users will have to wait for the release of 2.0.46 to get a fix for that problem, the ASF said.
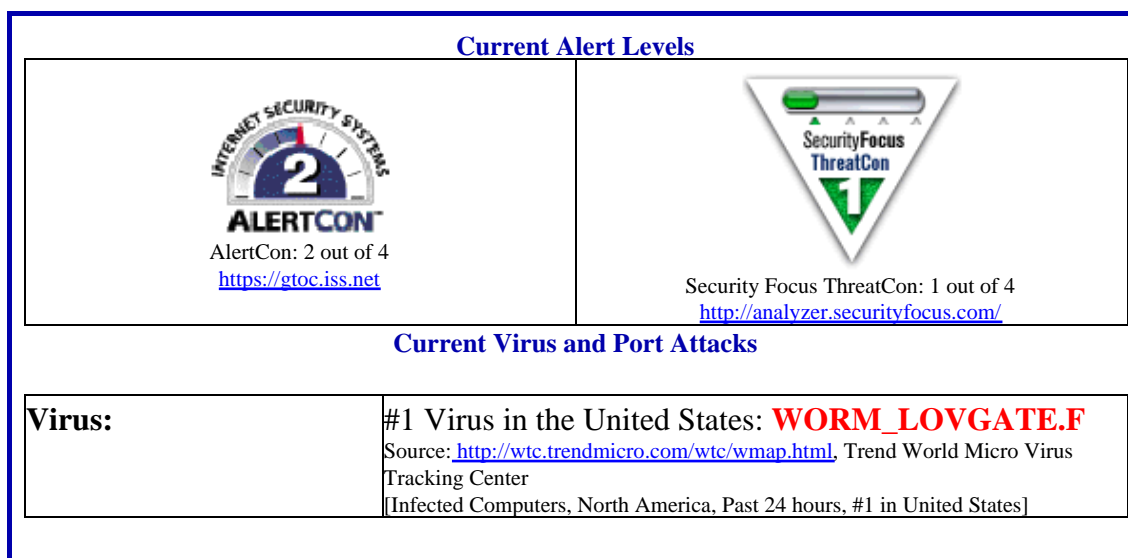Source: http://www.nwfusion.com/news/2003/0403newapach.html

21. *April 02, Security News Portal* — **75% of all web servers running MS IIS 5.0 are vulnerable to exploitation. Three–quarters of web sites running Microsoft's Internet Information Server 5.0 software to serve web pages have the WebDAV protocol enabled and thus remain open to a serious vulnerability which was announced by Microsoft last month**, the latest web server survey from Netcraft says. Microsoft issued a security alert on March 17 regarding a buffer overflow vulnerability which allows attackers to execute arbitrary code on Windows 2000 machines. **The survey found 767,721 IPs running IIS 5.0 and offering WebDAV and 273,496 IPs running IIS 5.0 with the protocol turned off**. The monthly survey looks at web server software usage on internet–connected computers, collecting and collating as many hostnames as can be found providing an HTTP service. Each is systematically polled with an HTTP request for the server name. The March survey received responses from 39,174,349 sites. Additional information may be found on the Netcraft Website: http://news.netcraft.com/archives/2003/03/
Source: http://www.securitynewsportal.com/cgi–bin/cgi–script/csNews/ csNews.cgi?database=JanY.dbid=67/TD>

Internet Alert Dashboard

Current Alert Levels	
AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]

Top 10 Target Ports	80 (www), 137 (netbios–ns), 1434 (ms–sql–m), 25 (smtp), 445 (microsoft–ds), 4662 (eDonkey2000), 36475 (–––), 139 (netbios–ssn), 113 (ident), 1214 (kazaa)
	Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

22. *April 05, New York Times* — **Britain moves to deport radical cleric.** Britain moved on Saturday to deport Abu Hamza al–Masri, the country's most outspoken radical cleric, who until recently was the imam of a mosque in North London widely depicted as a recruiting ground for fundamentalist Islam and al Qaeda. **David Blunkett, the home secretary, said on Saturday that he had sent Masri a letter withdrawing his citizenship and that Masri had 10 days to appeal or be deported.** Masri, 44, is an Egyptian–born former nightclub bouncer who has one eye and wears a hook where a hand was blown off by a land mine in Afghanistan 20 years ago. Newspapers and members of Parliament have increasingly called for his expulsion since evidence emerged that he persuaded young British Muslims to wage holy war against the West. **Blunkett's move to expel Masri was the first taken under new laws that came into effect Tuesday empowering the government to strip immigrants with dual nationalities of their British citizenship and deport them if their activities threatened the national interest.** Blunkett said the action against Masri was based on the cleric's having encouraged people "to take part in the jihad and fight us overseas."
Source: http://www.nytimes.com/2003/04/05/international/europe/05CND–BRIT.html

23. *April 04, Associated Press* — **Guilty plea paves way for testimony in terrorism case.** A key government witness in the case of an alleged "sleeper" terrorist cell pleaded guilty on Thursday to 10 federal charges of fraud and misuse of a visa, clearing the way for him to testify. **Youssef Hmimssa, 32, could testify next week in the trial that began late last month of four North African men accused of conspiring to provide material support or resources to terrorists. The government alleges that the four defendants attempted to recruit Hmimssa and wanted him to make false documents to get people into the country illegally.** Charges against Hmimssa and the others stem from a raid on a Detroit apartment six days after the Sept. 11, 2001, attacks. Prosecutors say the raid turned up a day planner that detailed planned attacks on a U.S. air base in Turkey and a hospital in Jordan, as well as a videotape of U.S. landmarks, including Disneyland and Las Vegas's MGM Grand Hotel and Casino. **Three of the conspiracy defendants –– Karim Koubriti, 24, Ahmed Hannan, 34, and Farouk Ali–Haimoud, 22 –– were arrested in Detroit at the time of the raid. Hmimssa was arrested later that month in Iowa, and the alleged handler of the cell, Abdel–Ilah Elmardoudi, 37, was arrested in November 2002 in North Carolina.**
Source: http://www.washingtonpost.com/wp–dyn/articles/A23453–2003Apr 3.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.